

# 3. Client Enrollment

Please follow each section that corresponds with the device types you want to enroll in FileWave.

You will notice that some device types, such as iOS and macOS, contain new information, while Windows and Chromebooks redirect to a previous section.

- [Android Enrollment](#)
- [Apple DEP Enrollment](#)
- [Apple Manual Enrollment](#)
- [Using LDAP to enroll macOS/iOS/Android devices](#)
- [Chromebook Enrollment](#)
- [Windows Enrollment](#)

## Enrolling Android devices to FileWave

There are several ways to enroll Android devices;

- ❗ Devices in Safe Mode may not be enrolled

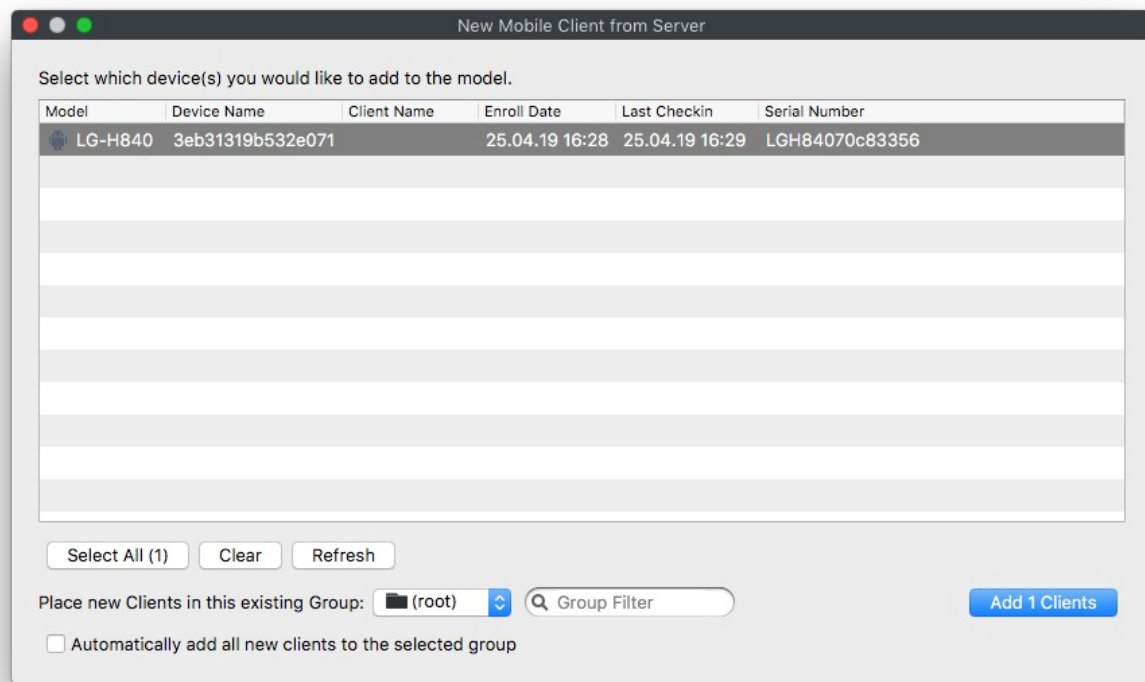
First create an enrolment token from the menu item: 'Assistants' > 'Enroll Android Device...'

[illegible]

- Tapping the screen seven times (in the same spot) or
- Entering `afw#setup` in place of a Google account.

On completion a summary will appear. Click Setup.

Where auto enrolment is configured in the New Client > Enrolled Mobile Devices, the device should appear within a few minutes. Otherwise use the New Client window to accept the device and then Update Model.



## Android BYOD (EMM)

Android BYOD (Bring Your Own Device) Enrollment, also known as Android Enterprise Work Profile, is a method of enrolling personal Android devices in an Enterprise Mobility Management (EMM) system. This allows organizations to manage and secure corporate data and apps on employees' personal devices, while maintaining user privacy and keeping personal data separate from work data.

In this enrollment method, a work profile is created on the user's personal device, which acts as a separate container for work-related apps and data. This ensures that the organization can only manage and access the work profile, without interfering with the user's personal data and apps.

Android BYOD Enrollment offers several benefits, such as:

1. Increased flexibility: Employees can use their personal devices for work, reducing the need for organizations to provide dedicated work devices.
2. Enhanced security: Corporate data is secured within the work profile, preventing unauthorized access and data leakage.
3. Improved privacy: Users maintain control over their personal data and apps, as the organization can only manage the work profile.
4. Simplified management: EMM administrators can easily manage and configure work profiles, apply policies, and distribute apps to enrolled devices.

To implement Android BYOD Enrollment, organizations need an EMM solution that supports Android Enterprise, such as FileWave. The EMM solution will guide users through the enrollment process and help administrators manage and configure work profiles on enrolled devices.

## Getting Started with BYOD (EMM)

**The very first step before getting start with BYOD (EMM) is to setup Android EMM using the start of this article.**





After going through the EMM setup, continue with the next steps.

1. Download Android device policy App ([https://play.google.com/store/apps/details?id=com.google.android.apps.work.clouddpc&hl=en\\_US](https://play.google.com/store/apps/details?id=com.google.android.apps.work.clouddpc&hl=en_US))
2. From the App scan the Enrollment QR code
3. Add the devices to admin as normal
4. (Observe) you will have a "Play Store" app and a "Work Play Store"

The devices will have the same icon in admin.

If the Inventory field "Is User-Owned" is True, the device is a BYOD.

I would add this as a column in the client view to more easily identify.

	3681592250960e8b	/- Inbox/Mobile/	Android	false	H/
	36f10c79dbea6608	/	Android	false	H/
	3b20d2c2020a123e	/	Android	true	H/
	Bam's FW iPad	/- Inbox/Mobile/	iOS		D/

**BYOD**

## Enrollment Workflow (EMM)

If you have a Google Policy Fileset with Network information in it. You can select it when you generate a QR code. This inserts the information onto the device for easy enrollment.

QR Code

Details

Enterprise

preview (LC013lb0yu) ⌵

Base Policy

Default Policy for preview (default) ⌵

Reusable

☐ Multiple enrollments
☒ Single-use only

Duration

30 ⌵

Days ⌵

WiFi Profile

(None) - (2907) My Network 1 ⌵

Comment

Create

Figure 1.1 - WiFi selected in enrollment QR

The QR code that is generated contains the WiFi password in plain text.

DO NOT leave the QR code just sitting around.

## Android EMM Location Tracking

Android EMM devices need to install a FileWave "companion" application onto the device that will send us location data. Reference [Force Location for EMM Android Devices](#) for details.





# Apple DEP Enrollment

## Benefits of DEP Enrollment

iOS, tvOS, and macOS can all take advantage of Apple DEP enrollment. DEP enrollments will force a specific set of preferences on the device and force enrollment to FileWave any time the device is Factory Reset. Another huge benefit of DEP is that DEP is the only enrollment option that prevents the end-user from removing the MDM Profile and unenrolling the device. These two aspects can be very helpful in device recovery situations since if the device is wiped after being lost or stolen, the device will automatically enroll back into FileWave where you can lockdown the device and collect Location Tracking information to report to the authorities.

If you have not already created your Apple Push Notification Service Certificate (APNS) or configured DEP to sync with FileWave, please review the [Platform Integrations > Apple Integration](#) section before continuing.

## Creating DEP Profiles

The first step to enrolling your Apple devices via DEP is to create a DEP Profile. The DEP Profile is what will determine the initial settings applied to the device during enrollment and applies to all Apple platforms. Unless needing explicit separation of the initial enrollment settings, one DEP Profile can suffice for all of your devices. This is partly possible since we can use FileWave Custom Fields to uniquely name the devices.

1. Open FileWave Admin and navigate to "Assistants > DEP Association Management".
2. Click the "[+]" button on the right-hand side under "Profiles".
3. Fill out each tab according to your management preferences.

Information	Options	Setup Assistant	Account	Anchor Certs	Supervising Certs	Device Naming	Activation Lock Management
-------------	---------	-----------------	---------	--------------	-------------------	---------------	----------------------------

ⓘ This information is optional but will display on devices when Locked or in Missing Mode.

- **Support Phone Number**
- **Support Email**
- **Department**

Information	Options	Setup Assistant	Account	Anchor Certs	Supervising Certs	Device Naming	Activation Lock Management
-------------	---------	-----------------	---------	--------------	-------------------	---------------	----------------------------

ⓘ These items are very crucial so please choose wisely.

- **Do not allow user to skip enrollment step** - Forces device to enroll into FileWave (**check recommended**)
- **Supervise** - Allows for full device management using Profiles (**check recommended**)
  - **Is MDM Removable** - Allows user to remove MDM Profile and unenroll device (**uncheck recommended**)
  - **Allow Pairing** - Allows pairing to iTunes (**optional**; can be restricted using Profile)
  - **Automatic Advance** - Applies only to tvOS (**optional**)
- **Enable Shared iPad** - Leave disabled unless planning to use Apple Classroom
  - **Number of users**

Information	Options	Setup Assistant	Account	Anchor Certs	Supervising Certs	Device Naming	Activation Lock Management
-------------	---------	-----------------	---------	--------------	-------------------	---------------	----------------------------

ⓘ Most users choose to disable all Setup Assistant items except for "Location Services" to speed up the initial setup.

- **Location Services** - Allows FileWave to do Location Tracking and set timezone automatically

Information	Options	Setup Assistant	Account	Anchor Certs	Supervising Certs	Device Naming	Activation Lock Management
-------------	---------	-----------------	---------	--------------	-------------------	---------------	----------------------------

ⓘ Applies only to macOS devices; at least one Administrator account must be created.

- **Prompt user to create an account type of:** - allows user to create account during macOS setup
- **Create managed macOS Administrator Account** - creates Admin account (**recommended**)

Information	Options	Setup Assistant	Account	<b>Anchor Certs</b>	Supervising Certs	Device Naming	Activation Lock Management
-------------	---------	-----------------	---------	---------------------	-------------------	---------------	----------------------------

ⓘ Skip this section; automatically configured.

Information	Options	Setup Assistant	Account	Anchor Certs	<b>Supervising Certs</b>	Device Naming	Activation Lock Management
-------------	---------	-----------------	---------	--------------	--------------------------	---------------	----------------------------

ⓘ Skip this section unless you'd like to manage iOS using DEP and Apple Configurator 2.

Information	Options	Setup Assistant	Account	Anchor Certs	Supervising Certs	<b>Device Naming</b>	Activation Lock Management
-------------	---------	-----------------	---------	--------------	-------------------	----------------------	----------------------------

ⓘ Uniquely names iOS, tvOS, and macOS device during DEP Enrollment.

- **Naming Policy** - Leave as default
- **Naming Template** - Field accepts plain text and variables including native device data and FileWave Custom Fields.

Information	Options	Setup Assistant	Account	Anchor Certs	Supervising Certs	Device Naming	<b>Activation Lock Management</b>
-------------	---------	-----------------	---------	--------------	-------------------	---------------	-----------------------------------

ⓘ Configures or disables Activation Lock for iOS and macOS.

- **Activation Lock Configuration**
  - Disabled - completely disables Activation Lock and FindMy
  - iCloud - Allows Activation Lock for any Apple ID
  - ASM/ABM (Organization) - Allows Activation Lock on for Managed Apple IDs
- **Allow Activation Lock only if Bypass Code is available** - Failsafe to ensure Bypass Code is stored in FileWave's encrypted databased (**recommended**)

## Assigning DEP Profiles

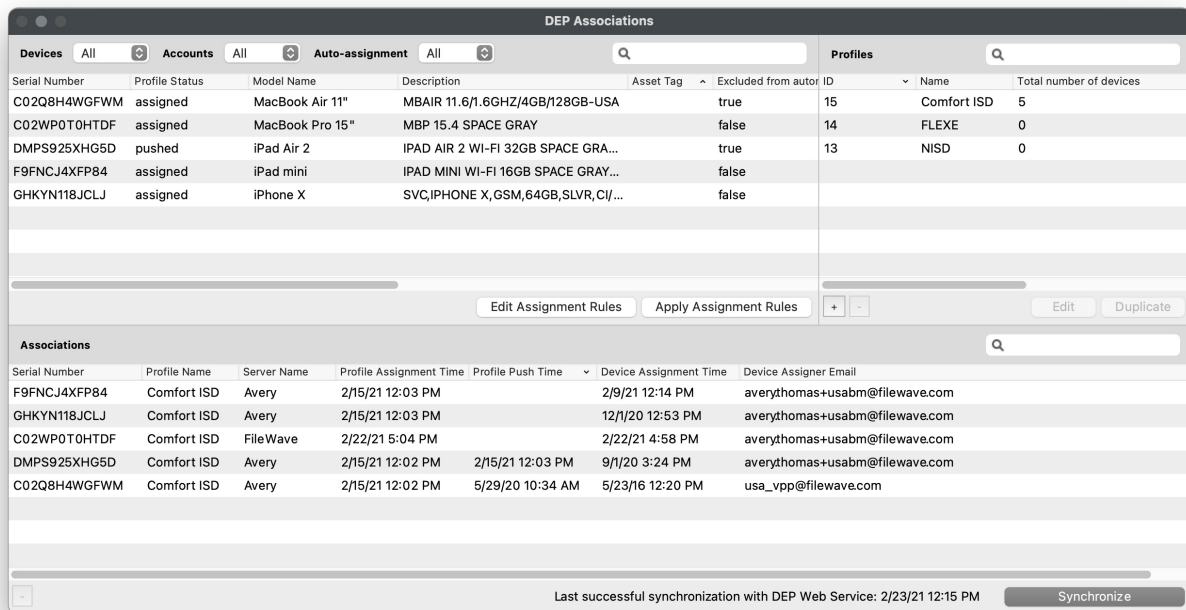
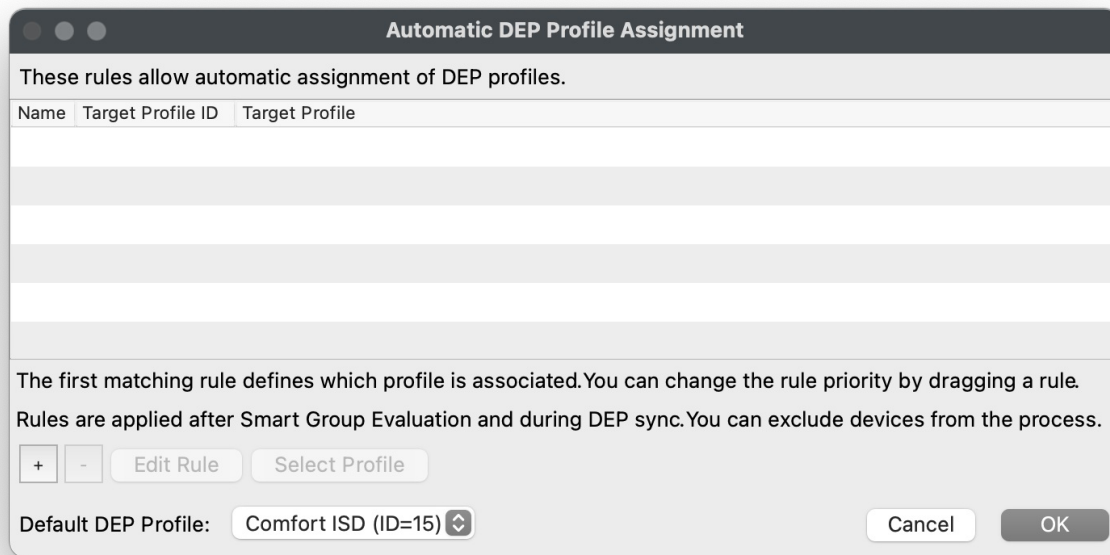
Assigning DEP Profiles is very easy within FileWave, especially if you only have one DEP Profile since you can set a Default DEP Profile. With a Default DEP Profile configured, anytime you assign a new device to the FileWave MDM Server from within Apple School Manager or Apple Business Manager, the DEP Profile will automatically apply and the device will be ready for DEP enrollment. However, if you have multiple DEP Profiles, FileWave will also enable you to create Rule-based DEP Profile assignments or you can always just drag-n-drop a DEP Profile onto a single device or multiple devices onto a DEP Profile.

The "Profile Status" field in the "Devices" pane tells you the current status of the DEP profile on the client device.

- Empty - no DEP Profile assigned
- Assigned - DEP Profile has been assigned but DEP enrollment has not occurred
- Pushed - Setup Assistant setting has run and settings have been enforced on client device
- Removed - DEP profile has been unassigned from device, will be changed to "Empty" after DEP sync

## Setting Default DEP Profile

1. Open FileWave Admin and navigate to "Assistants > DEP Association Management".
2. Click "Edit Assignment Rules".
3. Select your recently created DEP Profile from the "Default DEP Profile" dropdown menu.
4. Click "OK".
5. Click "Apply Assignment Rules" to save the changes.
6. Hold the Option or Alt key on your keyboard and click "Synchronize (full sync)" button in lower right-hand corner
7. You should now see that all of your devices have been "Assigned" to your DEP Profile.



## Rule-based DEP Profile Assignment

1. Open FileWave Admin and navigate to "Assistants > DEP Association Management".
2. Click "Edit Assignment Rules".
3. Click "[+]"
4. Select the DEP Profile you'd like to assign based on rules.
5. Drag-n-drop the Inventory data point the devices must meet to be assigned to the DEP Profile into the "Criteria" section.
6. Verify the criteria is correct by viewing the returned devices in the "Fields" section.
7. "Save" the query and "OK" to save rule definition.
8. Click "Apply Assignment Rules" to save the changes.
9. Hold the Option or Alt key on your keyboard and click "Synchronize (full sync)" button in lower right-hand corner.
10. You should now see that your selected devices have been "Assigned" to your DEP Profile.

Assignment Rule - Rule for NISD

Q

Component

Custom Fields

DEP Account

DEP Device

Asset Tag

Color

Description

Device Assigner Email

Device Assignment Time

Device Family

Excluded from automatic as...

Model Name

Operating System

Profile Assignment Time

Profile Push Time

Profile Status

Serial Number

The device's operating system:  
'iOS', 'OSX', 'tvOS'

Internal name: os

Name: Rule for NISD

Criteria

Fields

All of these expressions must be true

☐ Not DEP Device / Operating System

is

OSX

+

-

Add Group

Move up

Move down

Move in next group

Move before parent

Cancel

Save

Automatic DEP Profile Assignment

These rules allow automatic assignment of DEP profiles.

Name	Target Profile ID	Target Profile
Rule for NISD	13	NISD

The first matching rule defines which profile is associated. You can change the rule priority by dragging a rule. Rules are applied after Smart Group Evaluation and during DEP sync. You can exclude devices from the process.

+

-

Edit Rule

Select Profile

Default DEP Profile:

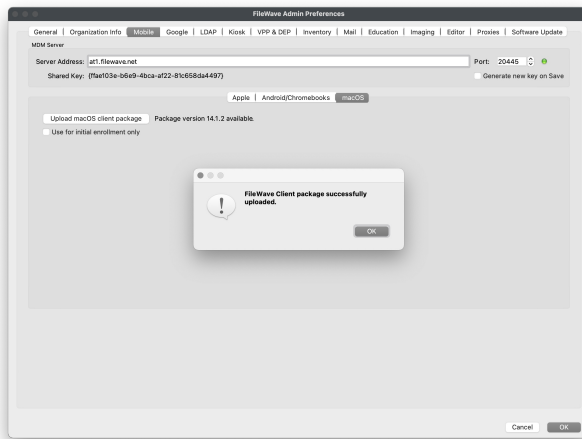
Comfort ISD (ID=15)

Cancel

OK

- ## Manually assign DEP Profile

- Sync Computer Name = macOS Hostname will be FileWave Client Name (recommended)
  - Server Name = Fully Qualified Domain Name of your FileWave Server
  - Server Port = 20015 (do not modify this as it will automatically go to the proper SSL port if you put in 20015)
  - Client Password = Password used to change individual Client Preferences and to start screen-sharing session
- Optional Settings
  - Is Tracking = Is Location Tracking Enabled for macOS Clients
  - Monitor Port = Port used for FileWave Client Monitor (do not modify)
  - Overwrite Configuration = Overwrite any existing FileWave Client configuration with settings entered here (recommended)
  - Remotecontrol Enabled = Screen-sharing enabled for Windows Clients
  - Remotecontrol Prompting = Whether or not to Prompt the end-user before starting screen-sharing session
  - Server Certificate = Only upload certificate is using a Self-Signed Certificate; not required for CA-signed certificate
  - Server Publish Port = 20005 (do not modify)
  - Tickle Interval = Idle time for Windows Clients before checking for new Model Update (do not modify)
  - Vnc Relay Port = 20030 (do not modify)
  - Vnc Server Port = 20031 (do not modify)
- Booster Settings
  - Do not configure unless instructed by FileWave SE



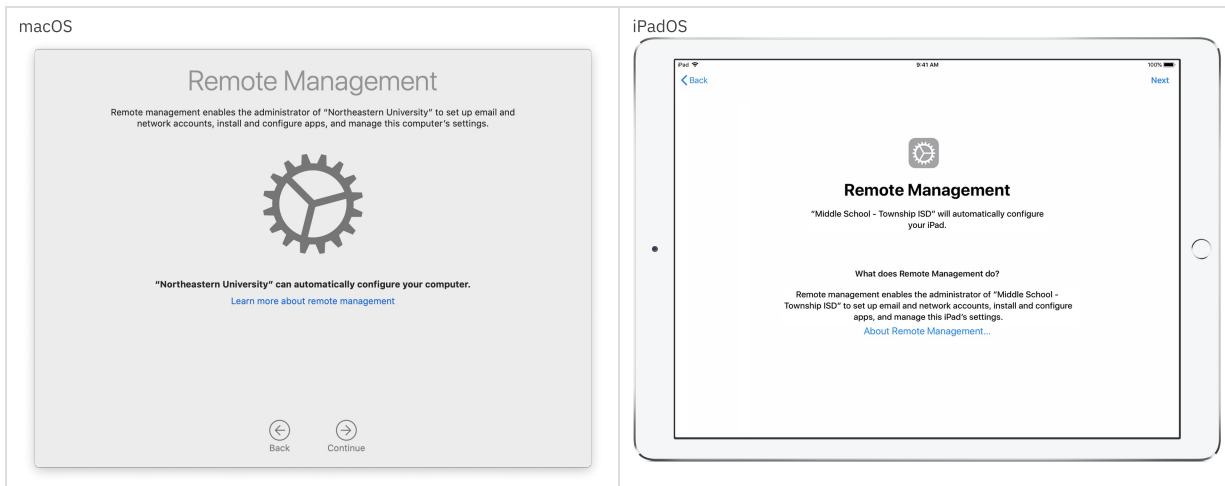
## Upload custom FileWave Client PKG to FileWave

1. Navigate to "FileWave Admin > Preferences > Mobile > macOS".
2. Click "Upload macOS client package" and authenticate.
3. Select the extracted "FileWaveClient\_XX.X.XX-FQDN-XX-XXX-XXXX.pkg" from previous section.
4. Wait for the upload confirmation prompt.
5. Optionally, enable "Use for initial enrollment only".
  - If this box is unchecked, FileWave will deploy any new FileWave Client version uploaded to all MDM enrolled macOS devices.
6. Click "OK" to save the Preferences.

## Enrolling Apple devices via DEP

Now that your devices have been "Assigned" to a DEP Profile, they can either be Factory Reset if already configured or taken fresh out of the box from Apple and they will automatically enroll into FileWave.

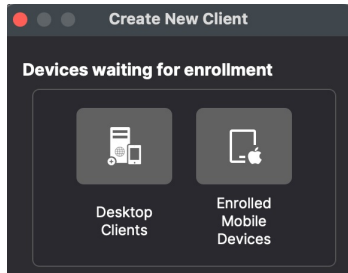
If getting authentication required during enrollment, please review [this](#) section to learn how to disable DEP enrollment authentication.



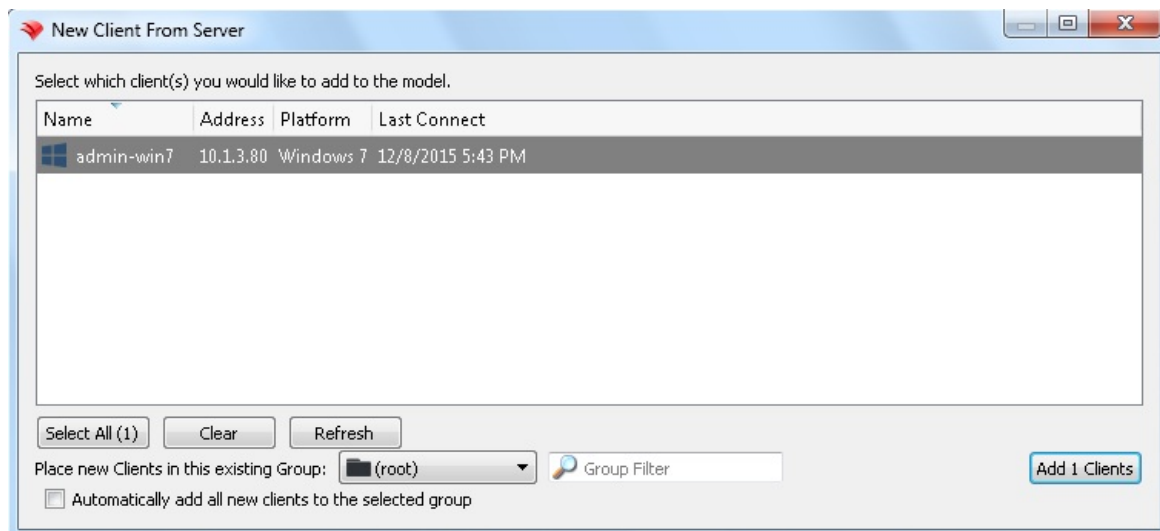


# Finalizing adding of clients


FileWave Clients communicating to the FileWave server will not be able to connect until you add them to the model. We will now allow our new client to join the FileWave server.



1. Open FileWave Central.
2. Click on the “New Client” button in the tool bar
3. Select either "Desktop Clients" or "Enrolled Mobile Devices" from the dialog box depending on whether it is a macOS or iPad.
4. Select your new client from the list presented.
5. Click the “Add Clients” button in the lower right.



Once you have selected “Add Clients”, you will be taken to the Clients view in FileWave Admin. By adding a client to the server, we have made changes to the model. In order for those changes to take effect, we need to perform a model update.

 You can also decide to automatically add new clients to skip the step of adding devices. This is discussed here: [Conflict Resolution](#)

## Making Changes to the Model

Remember that you will need to update the model anytime that you want to apply changes you have made. You can update the model after a single change or multiple changes (adding multiple clients, creating groups, etc.)

Congratulations! Your FileWave environment is now up and running! From here you can continue to add clients, build and deploy Filesets!



[illegible]

# Apple Manual Enrollment

## Not able to use DEP?

Apple's Device Enrollment Program is great but you may find that all or some of your devices aren't showing in [Apple School Manager](#) or [Apple Business Manager](#). Devices are usually excluded because they were not purchased directly from Apple or an Authorized Reseller. iOS device capable of running iOS 11+ can be manually added to your ASM/ABM account but unfortunately this not yet an option for macOS. This section covers several manual enrollment methods and why you might need to leverage them.

## Add iOS devices to ASM/ABM using Apple Configurator 2

If you have an iOS 11+ or tvOS 11+ device that was not originally purchased from Apple or an Apple Authorized Reseller, you can manually add the device to ASM/ABM using Apple Configurator 2. Please first review Apple's documentation [here](#) followed by FileWave Knowledge Base article [here](#) for more FileWave-specific processes. Once the device has been added to ASM/ABM you can take advantage of DEP for any future enrollments of this device.

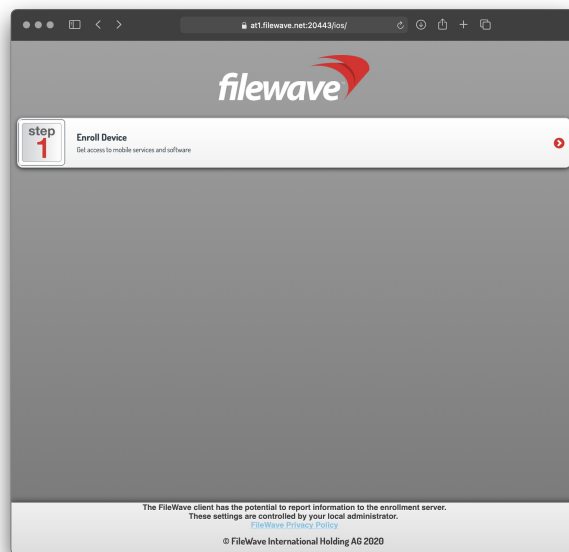
## MDM enroll iOS or macOS using URL Enrollment

If you are unable to enroll devices using DEP, you can still MDM enroll an iOS or macOS device using FileWave's URL Enrollment method. This method is commonly used to allow an end-user to MDM enroll a previously configured device without the need for a Factory Reset. The one downside to this enrollment method is that the end-user will have the ability to remove the MDM Profile and unenroll their device from the FileWave MDM. This process also requires the macOS users to have Administrator privileges in order to install the MDM Profile.

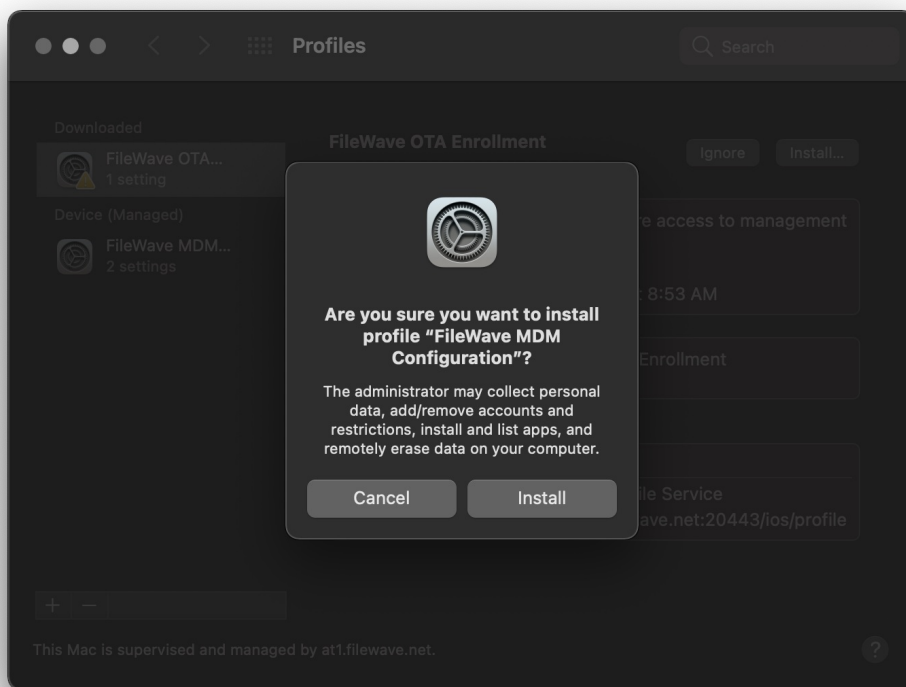
If getting authentication required during enrollment, please review [this](#) section to learn how to disable URL enrollment authentication.

### macOS URL Enrollment

1.

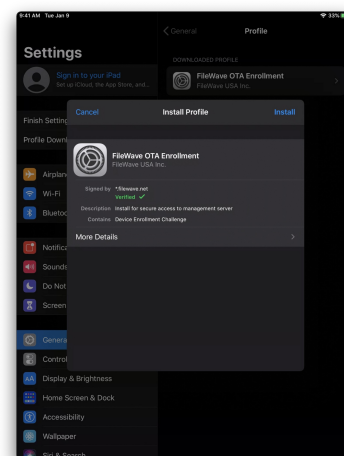
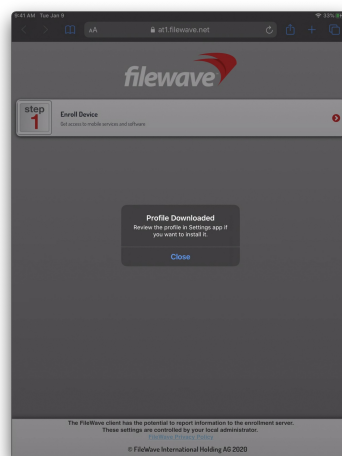
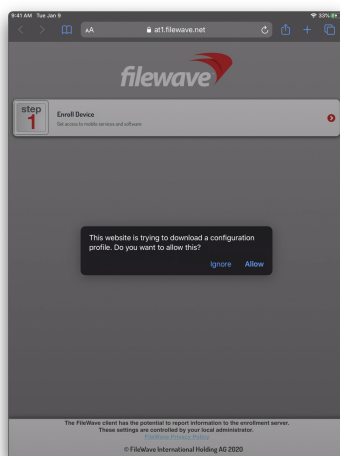


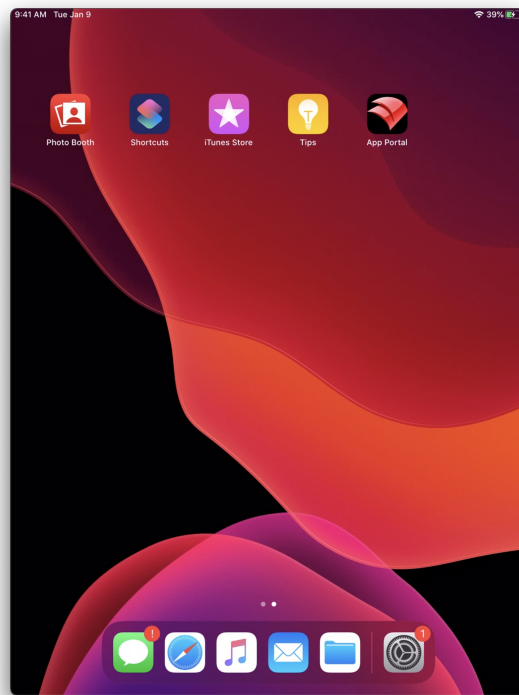
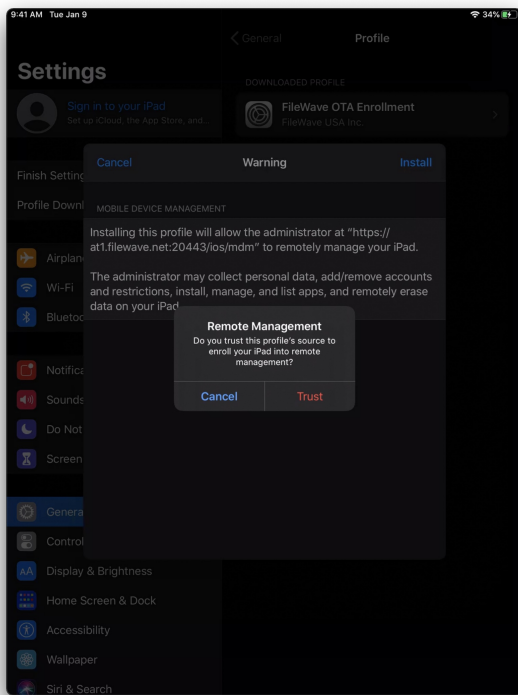
2. Navigate to "https://yourfilewaveserver.domain.com:20443" using web browser of choice.
3. Click the large "Enroll Device" button to download the MDM Enrollment Profile.
  - If using a self-signed certificate, you will see an additional step to download certificate.
  - If enrollment authentication is enabled, please authenticate.
4. Located the downloaded MDM Enrollment Profile "enroll.mobileconfig".
5. Double-click on the "enroll.mobileconfig" file.
6. Open "System Preferences > Profiles" from your macOS menubar.
7. Click "Install" next to the "FileWave OTA Enrollment" Profile.
8. Click "Install" again at the next prompt and authenticate using your macOS Administrator credentials.
9. The MDM Enrollment Profile is now installed and the FileWave Client will be installed automatically.
  - If you have not imported your custom macOS FileWave Client, please review the [Generate custom FileWave Client for macOS DEP enrollments](#) section.



## iOS URL Enrollment

1. Navigate to "https://yourfilewaveserver.domain.com:20443" using iOS Safari.
2. Click the large "Enroll Device" button to download the MDM Enrollment Profile.
  - If using a self-signed certificate, you will see an additional step to download certificate and [manually trust](#).
  - If enrollment authentication is enabled, please authenticate.
3. "Allow" the Profile download, acknowledge the "Profile Downloaded" prompt, and navigate to "Settings".
4. Click the "Profile Downloaded" item from the "Settings" and click "Install".
5. Click "Install" again and "Trust" the "Remote Management" prompt.
6. Your iOS device is now MDM enrolled and you should see the "FileWave App Portal" on the Home Screen.





## iOS User Enrollment (BYOD)

Starting with iOS 13, FileWave allows your end-users to enroll using User Enrollment. This is a new form of BYOD enrollment that allows your organization to deploy VPP applications to the devices while keeping other end-user data private from the MDM. This method also required the use of Managed Apple IDs configured in either Apple School Manager or Apple Business Manager.

For more in-depth information and setup of iOS User Enrollment, please consult the following FileWave Knowledge Base article [iOS BYOD User Enrollment](#). This article contains a video walk through of the enrollment process along with the [limitations](#) of iOS User Enrollment.

## Enroll non-MDM macOS Client

Enrolling a macOS device outside of the MDM is possible although it is unrecommended. To enroll a non-MDM macOS device into FileWave, you will need to simply install the FileWave Client PKG using a macOS Administrator account.

### Features unavailable with non-MDM macOS enrollment

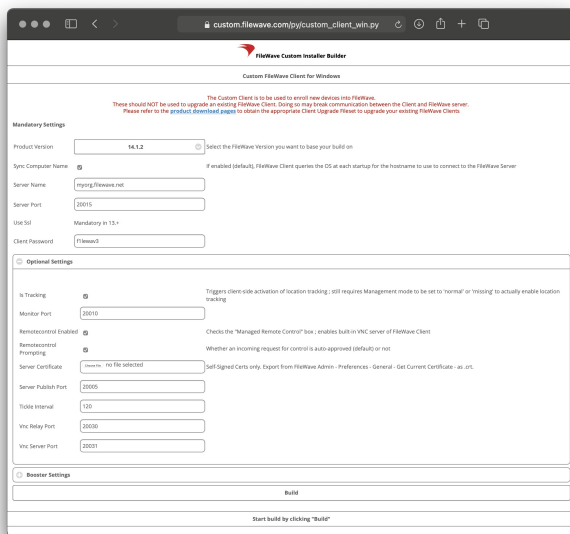
- VPP content deployment
- Profile Deployment (macOS Big Sur [unsupported](#))
- Profile Restrictions (Security and Privacy)
- FileVault Disk Encryption with Key Escrow
- Remote Shutdown/Reboot
- Lock Device
- Activation Lock Bypass
- Firmware Password Management
- Software Updates via MDM (macOS Big Sur)

### Features available with non-MDM macOS enrollment

- Location Tracking
- Fileset Deployment (PKG, .app, scripts)
- Limited Profile Restrictions
- Observe Client
- Remote Wipe
- Inventory w/ Custom Fields
- Legacy Software Updates

## Generate a custom FileWave Client PKG

- 1.



Open the [FileWave Customer Installer Builder](#) for macOS.

2. Fill out the settings accordingly.
3. Click the "Build" button and wait for the automatic download.
4. Extract ZIP and install the customized FileWave Client PKG.

#### Mandatory Settings

Product Version = Your FileWave Server Version

Sync Computer Name = macOS Hostname will be FileWave Client Name (recommended)

Server Name = Fully Qualified Domain Name of your FileWave Server

Server Port = 20015 (do not modify)

Client Password = Password used to change individual Client Preferences



Note: The default port setting for Server Port above is 20015. However, SSL is now required, and the system will automatically use port 20017 instead when 20015 is entered. Do not manually set the port to 20017. Always enter 20015, and the system will handle the SSL port change for you.

#### Optional Settings

Is Tracking = Is Location Tracking Enabled for macOS Clients

Monitor Port = Port used for FileWave Client Monitor (do not modify)

Overwrite Configuration = Overwrite any existing FileWave Client configuration with settings entered here (recommended)

Remotecontrol Enabled = Screen-sharing enabled for macOS Clients

Remotecontrol Prompting = Whether or not to Prompt the end-user before starting screen-sharing session

Server Certificate = Only upload certificate is using a Self-Signed Certificate; not required for CA-signed certificate

Server Publish Port = 20005 (do not modify)

Tickle Interval = Idle time for macOS Clients before checking for new Model Update (do not modify)

Vnc Relay Port = 20030 (do not modify)

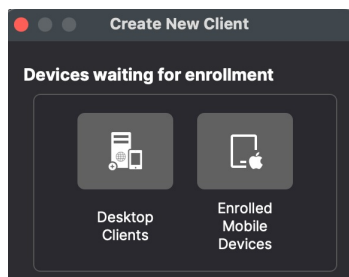
Vnc Server Port = 20031 (do not modify)

#### Booster Settings

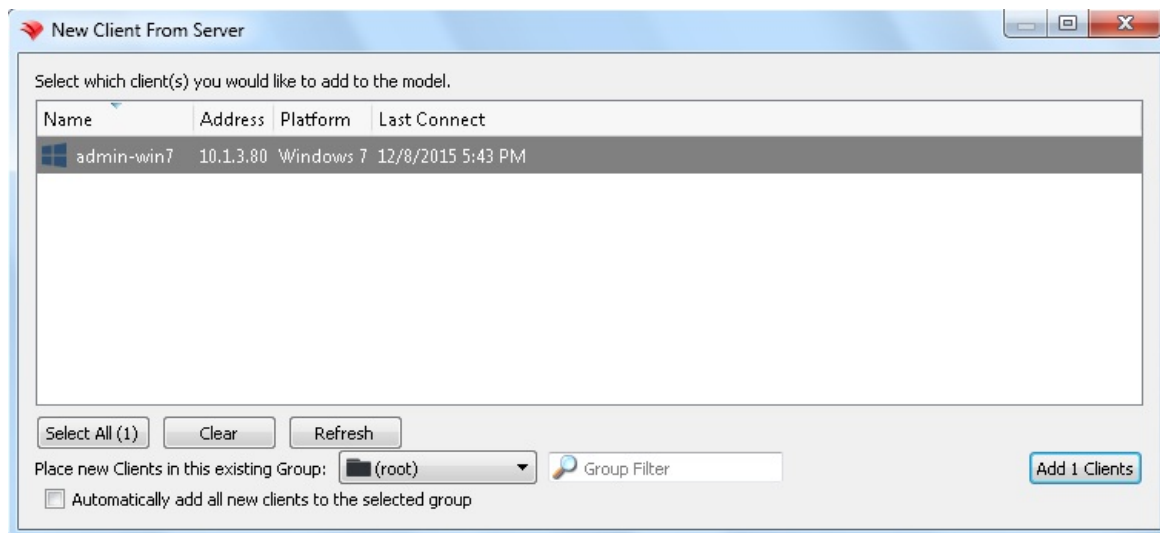
Initially you may want to make an installer that does not include Boosters. Read more about them here: [Boosters](#)

## Finalizing adding of clients

FileWave Clients communicating to the FileWave server will not be able to connect until you add them to the model. We will now allow our new client to join the FileWave server.



1. Open FileWave Central.
2. Click on the “New Client” button in the tool bar
3. Select either "Desktop Clients" or "Enrolled Mobile Devices" from the dialog box depending on whether it is a macOS or iPad.
4. Select your new client from the list presented.
5. Click the “Add Clients” button in the lower right.



Once you have selected “Add Clients”, you will be taken to the Clients view in FileWave Admin. By adding a client to the server, we have made changes to the model. In order for those changes to take effect, we need to perform a model update.

**i** You can also decide to automatically add new clients to skip the step of adding devices. This is discussed here: [Conflict Resolution](#)

## Making Changes to the Model

Remember that you will need to update the model anytime that you want to apply changes you have made. You can update the model after a single change or multiple changes (adding multiple clients, creating groups, etc.)

Congratulations! Your FileWave environment is now up and running! From here you can continue to add clients, build and deploy Filesets!

[illegible]

# Using LDAP to enroll macOS/iOS/Android devices

Use this document if you are trying to point your enrollment of device to directory services (Active Directory, Open Directory, eDirectory or OpenLDAP). This is used for Android Device and well as iOS devices or macOS devices enrolling OTA (over the air) as well as Apple's DEP (Device Enrollment Program) enrollment for both iOS and macOS devices.

This process consists of:

- 1- Backing up the current config
- 2- Editing a new config file to properly read the LDAP structure
- 3- Restarting the Apache Process so it reads the new config file

## Getting the files ready

Open a Terminal Window or use SSH to get into the computer running FileWave Server

Gain root credentials

```
sudo -s
```

Enter your login password

Navigate to the FileWave Apache configurations folder

OS X / Linux:

```
cd /usr/local/filewave/apache/conf/
```

Backup your current mdm\_auth.conf by making a copy

```
cp mdm_auth.conf mdm_auth.conf.bac
```

Make a copy of the LDAP example and rename it

```
cp mdm_auth.conf.example_ldap_auth mdm_auth.conf
```

## Making the changes

Open it up using your preferred text editor (nano mdm\_auth.conf or vi mdm\_auth.conf).  
it will look like this:

```
<Location /ios/enroll>
# This is an example of ldap based user auth
    AuthType Basic
    AuthBasicProvider ldap
    AuthName "Enroll IOS Device"
    AuthLDAPURL "ldap://10.1.10.25:389/cn=Users,dc=saturn,dc=filewave,dc=us?uid"
    Require valid-user
# If you need to bind to the ldap server, use these lines
#     AuthLDAPBindDN "cn=Admin,o=myorg"
#     AuthLDAPBindPassword "secret1"
    LDAPReferrals Off
</Location>

<Location /ios/dep_enrollment_profile>
# This is an example of ldap based user auth
    AuthType Basic
    AuthBasicProvider ldap
    AuthName "Enroll IOS Device"
    AuthLDAPURL "ldap://10.1.10.25:389/cn=Users,dc=saturn,dc=filewave,dc=us?uid"
    Require valid-user
    ErrorDocument 401 "Enrollment credentials are needed."
# If you need to bind to the ldap server, use these lines
#     AuthLDAPBindDN "cn=Admin,o=myorg"
```



```
#      AuthLDAPBindPassword "secret1"
      LDAPReferrals Off
</Location>

<Location /android/enroll>
# This is an example of ldap based user auth
  AuthType Basic
  AuthBasicProvider ldap
  AuthName "Enroll Android Device"
  AuthLDAPURL "ldap://10.1.10.25:389/cn=Users,dc=saturn,dc=filewave,dc=us?uid"
  Require valid-user
# If you need to bind to the ldap server, use these lines
#      AuthLDAPBindDN "cn=Admin,o=myorg"
#      AuthLDAPBindPassword "secret1"
      LDAPReferrals Off
</Location>

<Location /android/project_number>
# This is an example of ldap based user auth
  AuthType Basic
  AuthBasicProvider lda4
  AuthName "Google Cloud Messaging configuration"
  AuthLDAPURL "ldap://10.1.10.25:389/cn=Users,dc=saturn,dc=filewave,dc=us?uid"
  Require valid-user
# If you need to bind to the ldap server, use these lines
#      AuthLDAPBindDN "cn=Admin,o=myorg"
#      AuthLDAPBindPassword "secret1"
      LDAPReferrals Off
</Location>
```

The different sections correspond with the different enrollment URLs.  
For example, if my servers hostname was [server.filewave.com](https://server.filewave.com):

mdm\_auth.conf

URL	Use
<a href="https://server.filewave.com:20443/ios/enroll">https://server.filewave.com:20443/ios/enroll</a>	Over the air enrollment portal
<a href="https://server.filewave.com:20443/ios/dep_enrollment_profile">https://server.filewave.com:20443/ios/dep_enrollment_profile</a>	URL iOS or macOS Devices request when a DEP device is enrolling. This URL is not accessible from a normal browser.
<a href="https://server.filewave.com:20443/android/enroll">https://server.filewave.com:20443/android/enroll</a>	Downloading the APK FileWave Client
<a href="https://server.filewave.com:20443/android/project_number">https://server.filewave.com:20443/android/project_number</a>	Used by the FileWave Android client to talk to server

## Open Directory & eDirectory

OD (by default) does not require a user to authenticate to read the structure.  
You will not need to uncomment the bind options.

```
<Location /ios/enroll>
# This is an example of ldap based user auth
  AuthBasicProvider ldap
  AuthName "Enroll IOS Device"
  AuthLDAPURL "ldap://10.1.10.25:389/cn=Users,dc=saturn,dc=filewave,dc=us?uid"
  Require valid-user
# If you need to bind to the ldap server, use these lines
#      AuthLDAPBindDN "cn=Admin,o=myorg"
#      AuthLDAPBindPassword secret1
</Location>
```

**IP or URL** **What users in what group are allowed** **dn structure, usually url**

AuthName - The title of the login window  
AuthLDAPURL - Where and what groups are allowed to login and there for enroll. The example above would allow anyone in the 'Users' group to enroll a device.

Make the appropriate changes and then save the .conf

## Active Directory

AD (by default) requires you bind to the directory to read. Many people create a read-only directory account.

```
<Location /ios/enroll>
# This is an example of ldap based user auth
AuthType Basic
AuthBasicProvider ldap
AuthName "Enroll IOS Device"
AuthLDAPURL "ldap://192.168.1.96:389/cn=Users,dc=ad-ldap,dc=filewave,dc=com?sAMAccountName"
Require valid-user
# If you need to bind to the ldap server, use these lines
AuthLDAPBindDN "cn=TestDir Reader,cn=Users,ou=IT,dc=ad-ldap,dc=filewave,dc=com"
AuthLDAPBindPassword "Pa55W0rd"
</Location>
```

Annotations:

- dn structure, usually url (points to `dc=ad-ldap,dc=filewave,dc=com`)
- IP or URL (points to `192.168.1.96`)
- What users in what group are allowed (points to `cn=Users,ou=IT`)
- Exact location of Bind user (points to `cn=TestDir Reader`)
- Display Name of Bind user (points to `TestDir Reader`)

AuthName - The title of the login window

AuthLDAPURL - Where and what groups are allowed to login and there for enroll. The example above would allow anyone in the 'Users' group to enroll a device.

AuthLDAPBindDN - From specific to most general. Username, what group that is in, what group (or organizational unit) that group is in, and the server. The example above would allow the user 'TestDir Reader' who is in the group 'User' who is in the Org Unit 'IT' on the Active Directory server of [ad-ldap.filewave.com](http://ad-ldap.filewave.com) to bind.

AuthLDAPBindPassword - Password for user account being used to bind to AD.

Make the appropriate changes and then save the .conf

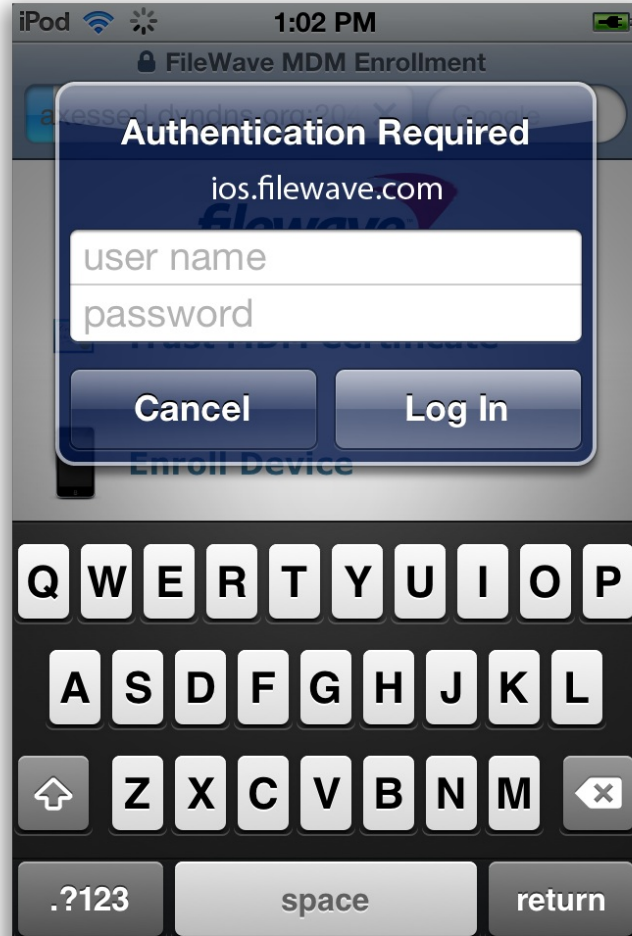
## Restarting Apache

Once saved, restart the FileWave Apache process/service

OS X / Linux:

```
/usr/local/filewave/apache/bin/apachectl graceful
```

Now when a device attempts to enroll (by pressing the Enroll Device option on the site). They will be prompted to enter their username and password from the directory server.



# Using several authentication sources for the same enrollment type

When we want to use several authentication sources (not nested locations) , we need to use AuthnProviderAlias sections to define those sources. The same format for binding to a single source ( see above ) apply for configuring each AuthnProviderAlias section , as in the following example

At the start of the file we define an alias by using:

```
<AuthnProviderAlias ldap ALIAS_NAME0>
  AuthLDAPBindDN ""
  AuthLDAPBindPassword ""
  AuthLDAPURL ""
</AuthnProviderAlias>
```

Then below that you specify the location and call for the alias

```
<Location /ios/enroll>
  AuthBasicProvider ALIAS_NAME0 ALIAS_NAME1 ALIAS_NAME2
  AuthType Basic
  AuthName "Enroll IOS Device"

  Require valid-user
</Location>
```

A final MDM\_auth.conf would look something like this:

```
<AuthnProviderAlias ldap Student>
  AuthLDAPBindDN "cn=BindUserName,dc=filewave,dc=net"
  AuthLDAPBindPassword "YourBindPassword"
  AuthLDAPURL "ldap://ldap.filewave.net:389/OU=student,dc=filewave,dc=net?sAMAccountName"
</AuthnProviderAlias>

<AuthnProviderAlias ldap Faculty>
  AuthLDAPBindDN "cn=BindUserName,dc=filewave,dc=net"
  AuthLDAPBindPassword "YourBindPassword"
  AuthLDAPURL "ldap://ldap.filewave.net:389/OU=staff,dc=filewave,dc=net?sAMAccountName"
</AuthnProviderAlias>

<Location /ios/enroll>
  AuthBasicProvider Faculty Student
  AuthType Basic
  AuthName "Enroll IOS Device"

  Require valid-user
</Location>
```

## Troubleshooting tips

Take a look at the log files for apache:

OS X / Linux:

```
<br>/usr/local/filewave/apache/logs/error_log<br>
```

Below are some sample errors and what they typically mean.

NOT Bound:

```
[Thu Feb 09 22:10:19 2012] [error] [client 192.168.1.109] user diradmin: authentication failure for "/ios/enroll":
Password Mismatch, referer: https://192.168.1.95:20443/ios/
```

Bound but user entered info wrong OR ldap url pointed to wrong group:

```
[Thu Feb 09 22:29:16 2012] [error] [client 192.168.1.109] user diradmin: authentication failure for "/ios/enroll":
Password Mismatch
```

Bound w/ Bad User

```
[Thu Feb 09 22:29:00 2012] [error] [client 192.168.1.109] user lkajshdg not found: /ios/enroll
```

Could be Bound or not but not filtering by the correct ?uid?sAMAccountName at end of URL (?UID is an OD or eDir, AD is typically ?sAMAccountName)

```
[Thu Feb 09 22:17:31 2012] [error] [client 192.168.1.109] user admin not found: /ios/enroll, referer: https://192.168.1.95:20443/ios/
```

Something wrong in the mdm\_auth.conf file. Like AuthzLDAPAuthoritative isn't off or shouldn't be there.

```
apache require directives present and no authoritative handler
```

## Recursive issues

Does it appear that your server only looks at the one group/unit pointed to and not sub-groups? try adding ?sub at the end of your AuthLDAPURL lines:

```
AuthLDAPURL "ldap://ldap.filewave.net:389/OU=student,dc=filewave,dc=net?sAMAccountName?sub"
```

Always feel free to contact support for further assistance.

# Chromebook Enrollment

## How to enroll Chromebooks into FileWave

If you haven't already, please consult the [Platform Integrations > Chromebooks](#) section to learn how to sync Google Admin Console with FileWave. Once this sync has completed, all of your "Provisioned" Chromebooks will automatically appear in your FileWave Admin. No need for any additional enrollment process.

### Provisioning Chromebooks

Fortunately, provisioning Chromebooks is somewhat simpler than the configuration.

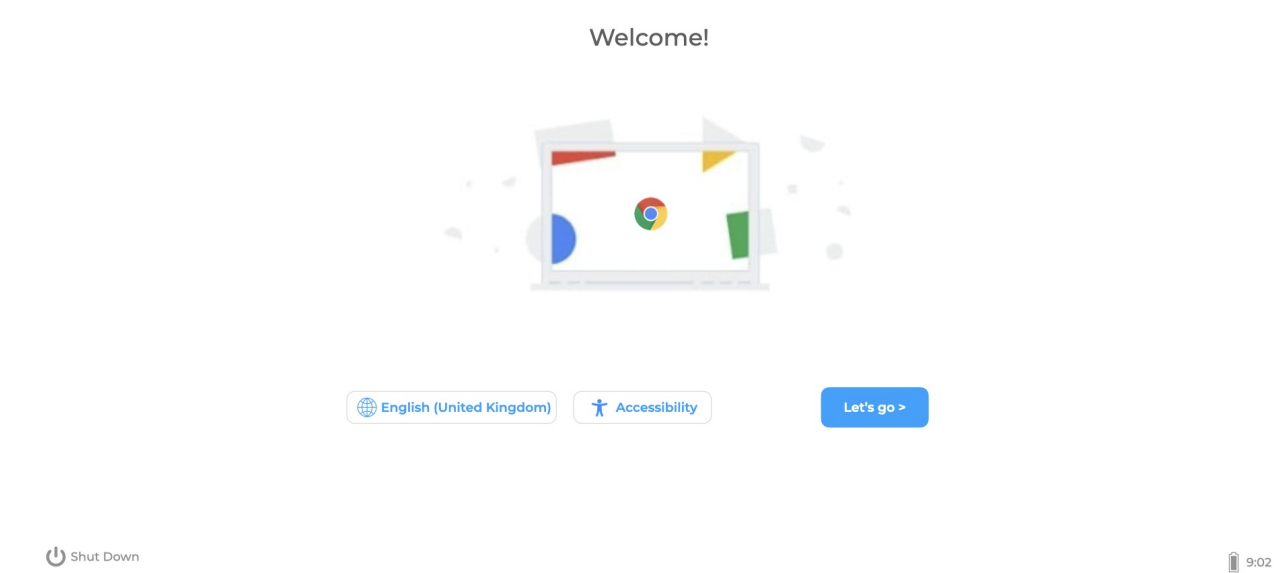


Do not log into the Chromebook before enrolment. Doing so, will require resetting the device and starting the process from scratch



A configured Google Enrolment user will be required to enrol the device

On power up, the device should present the Welcome page:



Click 'Let's go' and then select a Wi-Fi to join.

Once the device has joined a network, the device might show an Enterprise Enrolment page:



# Enterprise enrolment

[Learn more](#)

[Forgot email?](#)

Next

[< Back](#)

Shut Down

9:05

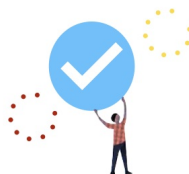
If not, select CTRL ALT E to enrol the device. Enter the Google Enrolment username and password.

The device will provide a bar showing enrolment is taking place. On completion a success page should be displayed:



**You are enrolled successfully**

You are enrolled successfully



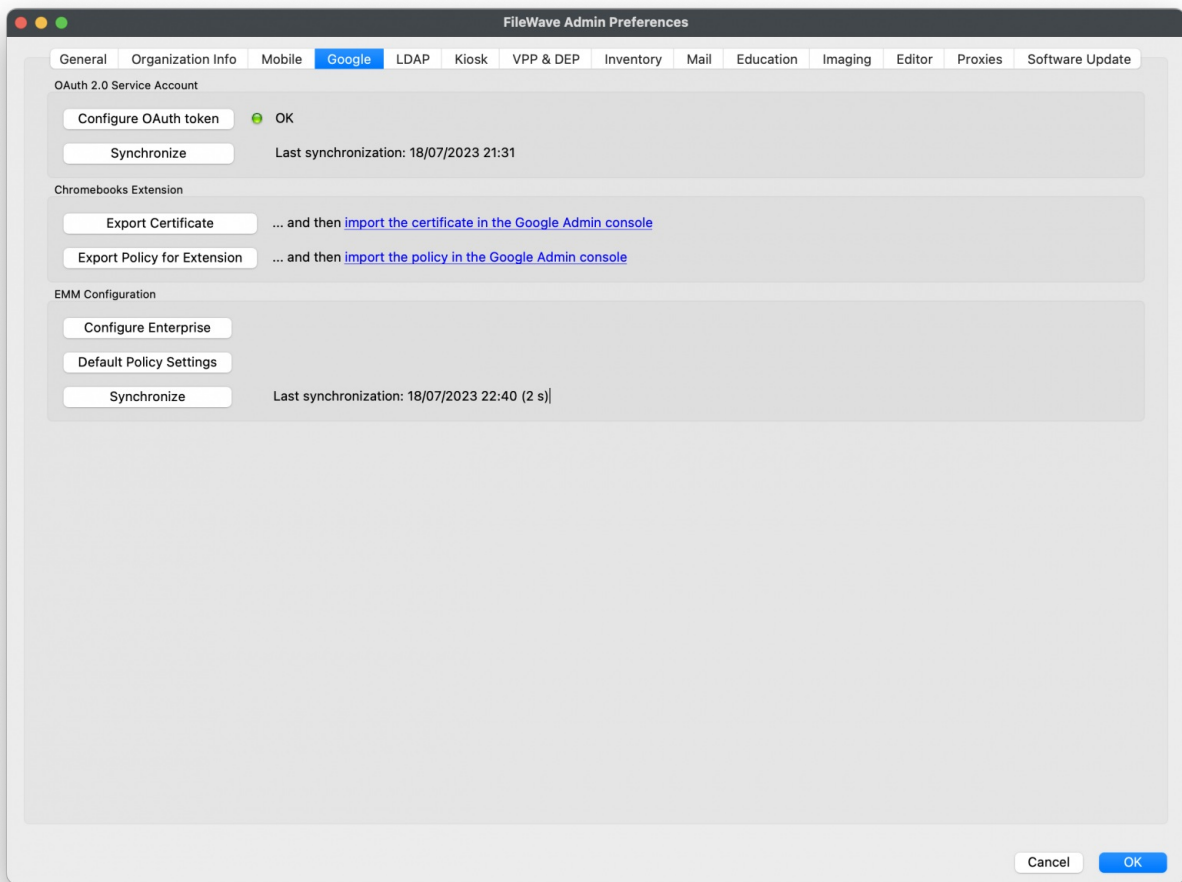
Done

Shut Down

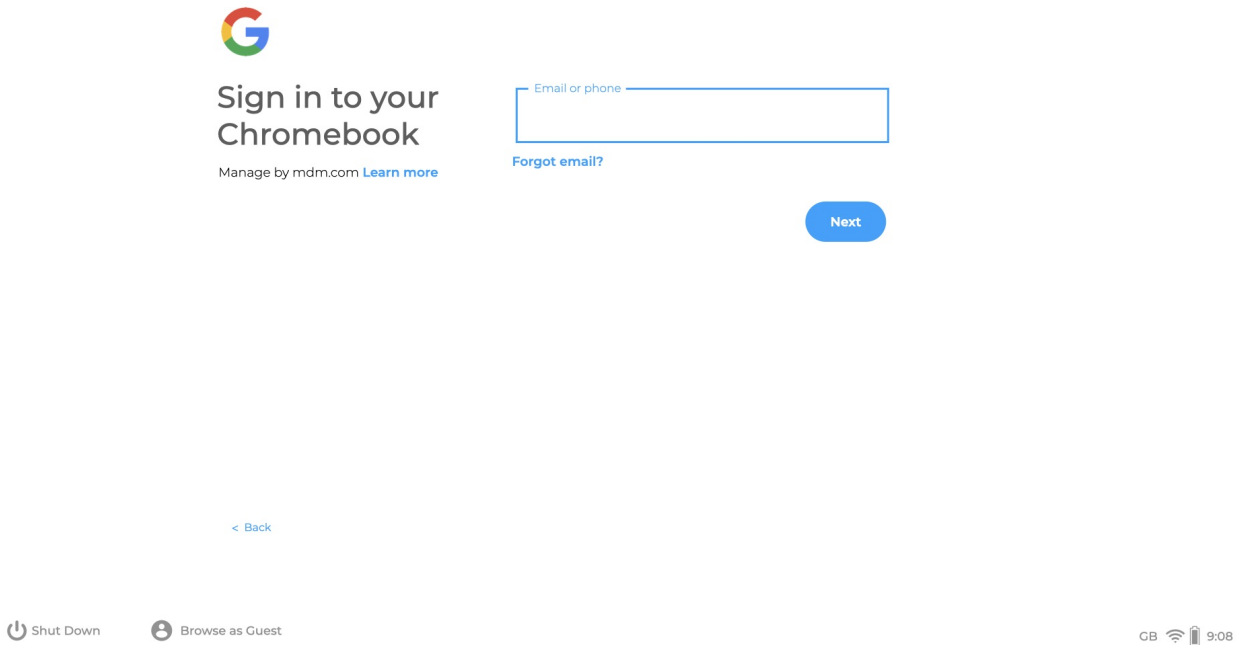
9:08

At this point the device should show in the Google Admin Console as a Provisioned device. On next FileWave, Google, OAuth synchronisation, the device should appear in the FileWave Client view.

Synchronisation may be triggered manually from the FileWave Central preferences:



Clicking 'Done' on the device should present the login page to the user:

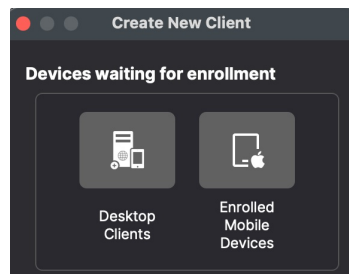


# Windows Enrollment

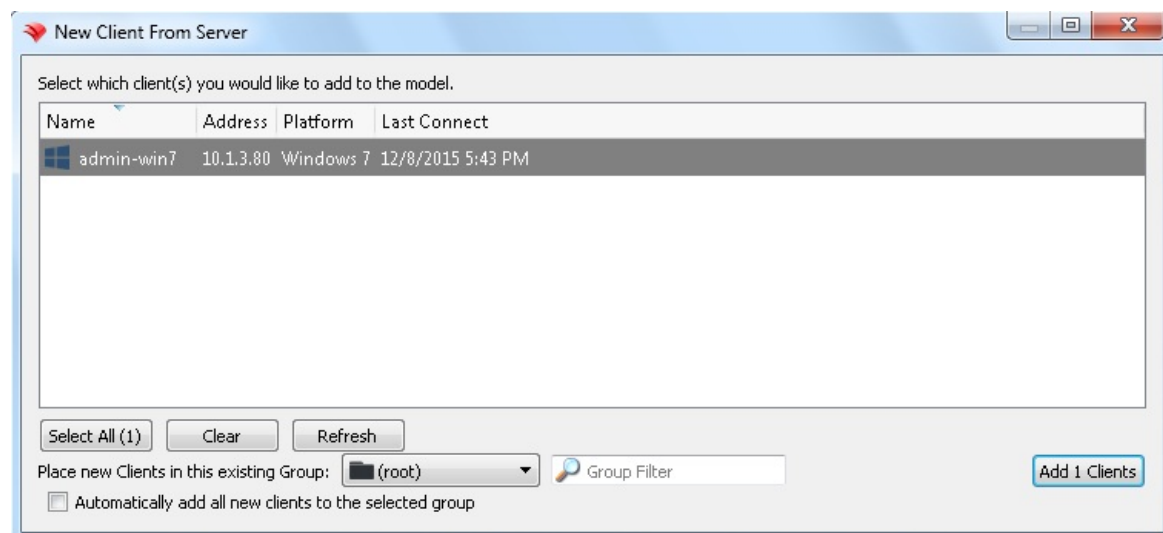
## How to enroll Windows Clients into FileWave

If you haven't already, please consult the [Platform Integrations > Windows](#) section for guidance on how to install the Windows FileWave client. If your organization uses Microsoft Entra ID and your users authenticate using Microsoft Entra ID credentials into their Windows machines, please consider enrolling your Windows machines into FileWave via Microsoft Entra ID. This will also allow for Windows MDM management within FileWave. Learn more on our [Windows MDM](#) article.

FileWave Clients communicating to the FileWave server will not be able to connect until you add them to the model. We will now allow our new client to join the FileWave server.



1. Open FileWave Central.
2. Click on the "New Client" button in the tool bar
3. Select either "Desktop Clients" or "Enrolled Mobile Devices" from the dialog box depending on whether it is a macOS or iPad.
4. Select your new client from the list presented.
5. Click the "Add Clients" button in the lower right.



Once you have selected "Add Clients", you will be taken to the Clients view in FileWave Admin. By adding a client to the server, we have made changes to the model. In order for those changes to take effect, we need to perform a model update.

**i** You can also decide to automatically add new clients to skip the step of adding devices. This is discussed here: [Conflict Resolution](#)

## Making Changes to the Model

Remember that you will need to update the model anytime that you want to apply changes you have made. You can update the model after a single change or multiple changes (adding multiple clients, creating groups, etc.)



[illegible]